WAM Class for Developers

OFFICE OF
ENVIRONMENTAL
INFORMATION

Lesson 1: Welcome and Course Overview

OFFICE OF
ENVIRONMENTAL
INFORMATION

Overview

- Purpose of the course
- Introductions
- Logistics
- Review course syllabus

Purpose of the Course

- To provide an understanding of:
  - The EPA Enterprise Identity and Access management (WAM) System
  - The process for Integrating an application into EPA Enterprise WAM System
- At the end of the course, students shall:
  - Be able to integrate an application into WAM System for enterprise Single Sign-on
  - Be able to integrate an application into WAM System using WAM Web services
  - Be a part of EPA's WAM Development Community

ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

Introductions

- Teachers
- Students
  - Who are you?
  - What is your background?
  - What do you want to get out of this training?
  - What do you like best about Spring?

Logistics

- One day course
- Parking is not covered by the class
- Start at 9am and ends around 5pm
- There will be one break in the morning and one in the afternoon
- Lunch: On your own

Course Syllabus Review—Day 1

- Welcome and Course Overview
- WAM in the Enterprise Architecture
- WAM Concepts and Definitions
- The EPA Enterprise WAM System
- The EPA Enterprise WAM Architecture
- The EPA WAM System in production
- Standards and compliance
- The EPA WAM Integration Process

Course Syllabus Review—Day 1

- EPA WAM and EPA Portal together
- Lab
- Course Wrap-up

Lesson 2: WAM in the Enterprise Architecture

OFFICE OF ENVIRONMENTAL INFORMATION

Vision for WAM at the EPA

- Until recently, there wasn’t an OTOP vision for WAM at EPA

- In joint EDSD/NCC discussions on April 19, 2006, the following vision statement was created:
    - Each user of EPA resources has a single, distinct, identity
    - Each resource will use the user’s single, distinct identity to provide services
    - The identity must be created and deleted by an authoritative source

Vision for WAM at the EPA (cont)

- There is a real need for providing a better solution for remote access to all Agency resources
- Program Offices need to collaborate without duplicating data and systems in both the private and public networks and without costly remote access solutions

People/Groups Involved with WAM

- EPA Staff
  - Maja Lee: WAM Portfolio Manger
  - Jody Zeugner: Security Architect
  - Mike Cullen: Program Management Officer
- EPA Groups
  - PMO: Coordinates WAM Activities
  - EDSD: Owner of the source information that populates WAM
  - OARM: Owner of the Human Resources source systems
  - NCC: Oversees the operations and hosting of the WAM system
- Contractors
  - SRA: Collects and tracks requirements for changes to the WAM system
  - Lockheed Martin: Designs and implements changes to the WAM system
  - CSC: Operates and maintains the WAM system

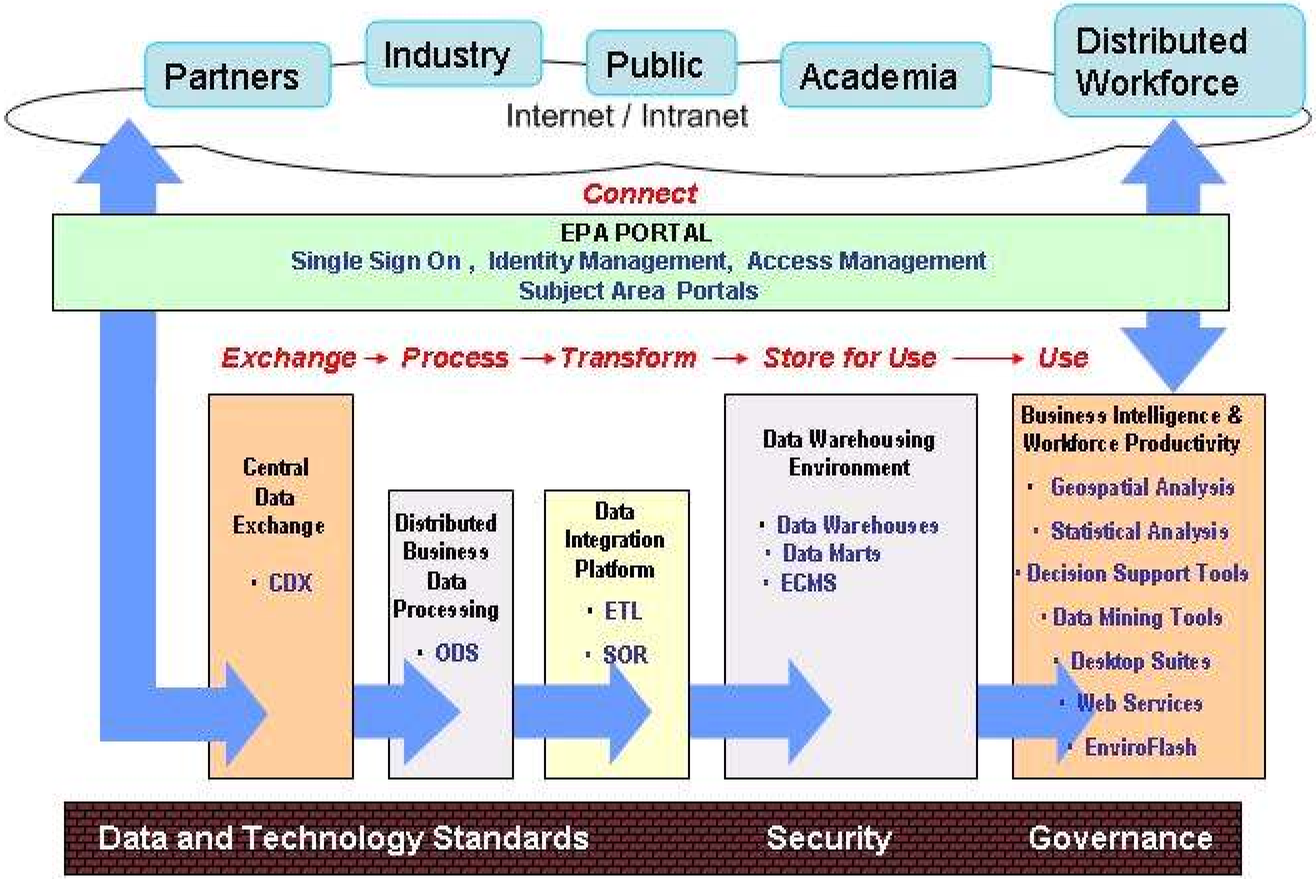
WAM Governance Board

- The WAM Governance Board currently includes representatives from the following organizations:
  - Program Management Office (PMO)
  - National Computer Center (NCC)
  - Program Offices (ORD)
  - Business Objects (BO)
  - Criminal Investigations Division (CID)
  - Mission Investment Solutions Division (MISD)
- However, it should be expanded to include:
  - Office of Acquisition Resource Management (OARM)
  - Enterprise Desktop Services Division (EDSD)
  - Office of Information Collection (OIC)

Enterprise Target Application Architecture

Target Applications Architecture:

Modernization Blueprint focused on Data Integration



Partners — Industry — Public — Academia — Distributed Workforce

Internet / Intranet

Connect

EPA PORTAL
Single Sign On , Identity Management, Access Management
Subject Area Portals

Exchange → Process → Transform → Store for Use → Use

Central Data Exchange
- CDX

Distributed Business Data Processing
- ODS

Data Integration Platform
- ETL
- SOR

Data Warehousing Environment
- Data Warehouses
- Data Marts
- ECMS

Business Intelligence & Workforce Productivity
- Geospatial Analysis
- Statistical Analysis
- Decision Support Tools
- Data Mining Tools
- Desktop Suites
- Web Services
- EnviroFlash

Data and Technology Standards — Security — Governance

Lesson 3: WAM concepts and Definitions

OFFICE OF ENVIRONMENTAL INFORMATION

It’s All About Identity…

“On the Internet, nobody knows you’re a dog.”

Source : Peter Steiner, July 5, 1993
The New Yorker (Vol. 69, No. 20)

What is Identity and Access Management?

- *“All the processes and technologies that manage the complete security and identity lifecycle for people and network entities in an organization*.“
  - Mary Ann Davidson, CSO of Oracle

- “*The business processes and supporting infrastructure for the creation, maintenance, and use of digital identities. The technical components of IdM include directories, meta-directories, provisioning, access management, single sign-on (SSO), password management, user administration, authentication mechanisms, and other technologies*.”

  - The Burton Group

Important Concepts

- **User Management** – The act of controlling user identities, including:
  - **Provisioning** – The mechanism by which a person establishes an identity. A user can establish their own identity (unverified users) or they can be given an identity by EPA (verified users)
  - **Maintenance** – Methods by which data about a person is updated as required (e.g. name changes)
  - **Deprovisioning** – Methods by which a person’s identity is revoked (e.g. termination of employment)

Important Concepts (cont)

- Authentication – The process by which a user proves that a given identity belongs to them, including:
  - Knowledge-based: Passwords and Secret Questions
  - Possession-based: RSA Tokens and Private Key Infrastructure (PKI) Certificates
  - Characteristic-based: HSPD-12 fingerprints

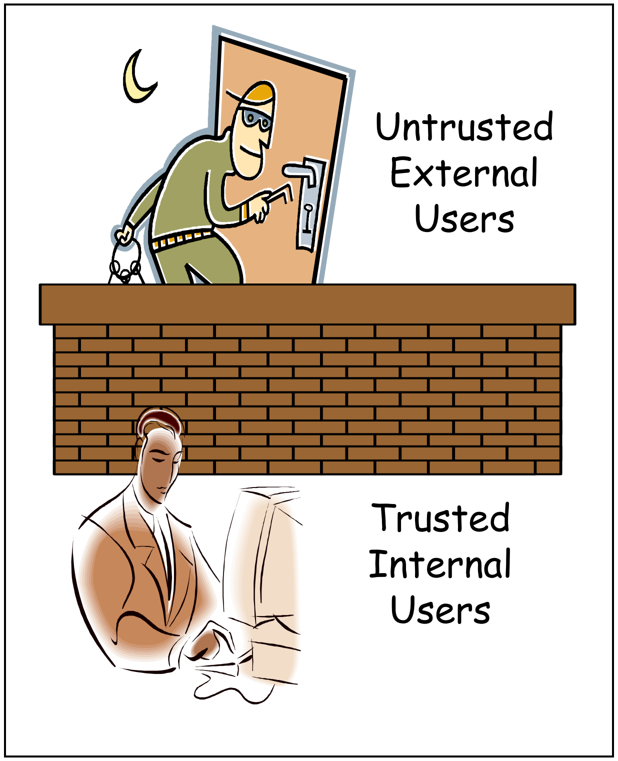
- Having different mechanisms from the same category is generally not more secure (e.g. multiple passwords)

- Having different mechanisms from different categories is more secure (e.g. password & RSA Token)

Important Concepts (cont)

- **Authorization** – The process of granting access for a specific resource, including:
  - Granting access to specific users
  - Placing users in groups and granting access to those groups
  - Granting access based on specific information about them (e.g. anyone working in Washington, DC)
  - Granting access based on where a user accesses the resource from (e.g. remote access users)

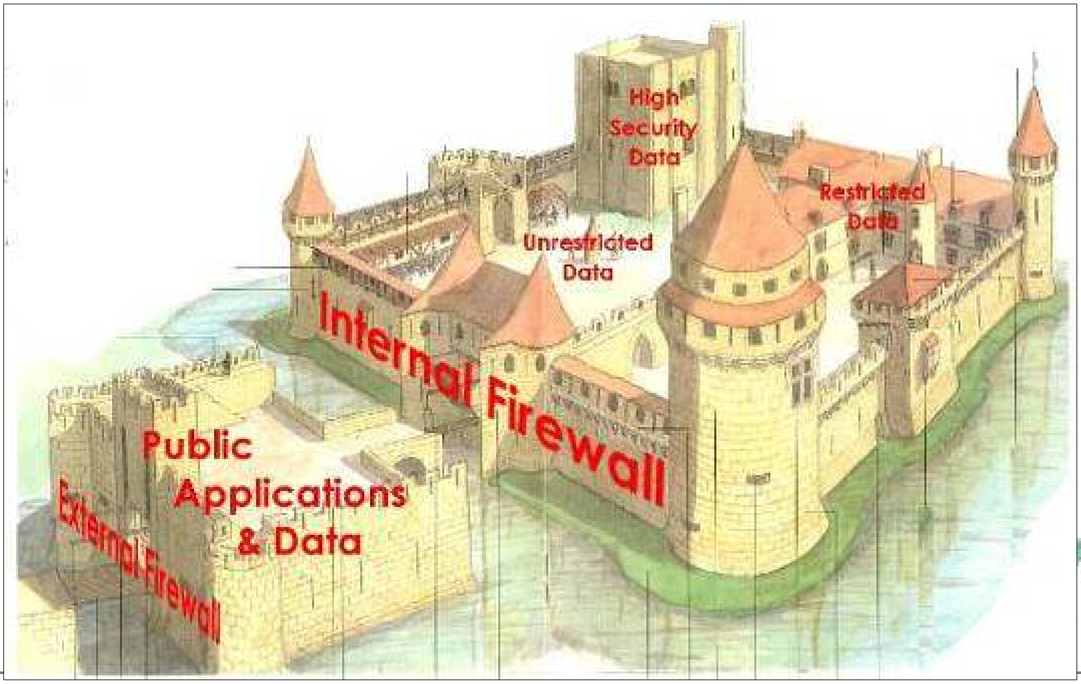
Current EPA Perimeter Control



- EPA users are classified broadly into trusted internal users and untrusted external users:
  - Internal users include anyone accessing EPA systems from a EPA network computer
  - External Users include anyone accessing EPA systems from outside the EPA network
- Access control is based on where someone is, not who they are, reducing collaborative opportunities, including
  - Emergency First-Responders cannot access information about facilities they are responding to
  - EPA staff working at home cannot access systems necessary to be productive
  - Contract System Designers cannot see information on the EA, development standards, Program Office business cases, etc.
  - Academia cannot locate data sets held by EPA when doing research
- AAA accounts require significant investment, user training, and set-up prior to use, reducing their effectiveness for large-scale solutions and emergency response

Perimeter Security Model

- Users should be allowed access to information based on who they are and how much we trust their authentication method:
  - Users remain in the Public Applications & Data zone
  - Requests for data are transported by the Portal across the Internal Firewall
  - Requests for more restricted data require more secure authentication methods
  - Removes the need for custom firewall rules for each application inside the internal firewall



ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

Terminologies

- Identity Management
  - Manages user information that is often distributed among multiple systems and technologies
- Access Management
  - Controls the user access to enterprise resources (i.e. URLs, EJBs, servlets)
  - Provides user and group management, delegated administration and password management
- Delegated Administration
  - The decentralization of role based access control systems
- Single Sign-on
  - Enables a user to authenticate once and gain access to the resources of multiple software systems.

ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

Lesson 4: The EPA Enterprise WAM System

What is EPA Enterprise WAM?

A shared, centrally managed infrastructure that provides identity and access management services to EPA applications via,

- An integrated, optimally designed Enterprise directory infrastructure storing identities of all users of EPA information systems. Includes
  - An LDAP-compliant “WAM Directory” – stores identities of all users of (participating) applications, including “extranet” users;
- Set of user identity administration tools, can be used by application managers to
  - Develop registration/approval apps/processes and
  - Manage identity data within the centralized directory infrastructure in delegated, distributed fashion

What is EPA Enterprise WAM? (Continued)

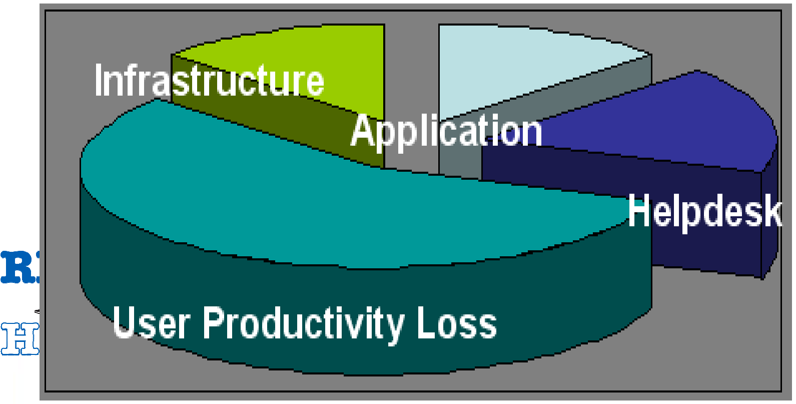
- **Directory integration/synchronization tools and processes that ensure**
  - Identity data is consistent across the component directories of the directory infrastructure and
  - Identity is created or deleted only by designated authoritative sources
- **An access management infrastructure that**
  - Provides applications policy-based access management services, including authentication, authorization, and Single Sign-On (SSO)
  - Provides these functions for application-to-application interactions (web services) as well as user-to-application interactions

What is EPA Enterprise WAM? (Continued)

- EPA Enterprise WAM will:
  - Enhance security
  - Substantially reduce overall administration costs
  - Accelerate application development and deployment
  - Reduces overall application development cost
- EPA Enterprise WAM will improve user experience by:
  - Reduction in number of discrete identities
  - Self-service registration and password management
  - Reduced/single sign-on

What are business drivers for WAM?

- Infrastructure hosting, including software licensing
  - Each identity system needs additional server/storage space and administration from NCC.
- Helpdesk support [1]
  - 25% help desk calls are password or user id related; each call costs $25 ~ $30
  - For 10,000 person organization, it costs around $135,000 ~ $270,00 per year.



- Application development and maintenance labor
  - Each application redevelops and maintains its own code for identity management
  - For 10,000 users and 20 applications, it costs 10,000 hours/year (or 5 FTEs)
- User productivity loss
  - Each user spends 16 minutes for login per day [2]
  - For 10,000 person organization, it costs about 2,666 hrs/day and 977,000 hrs/year

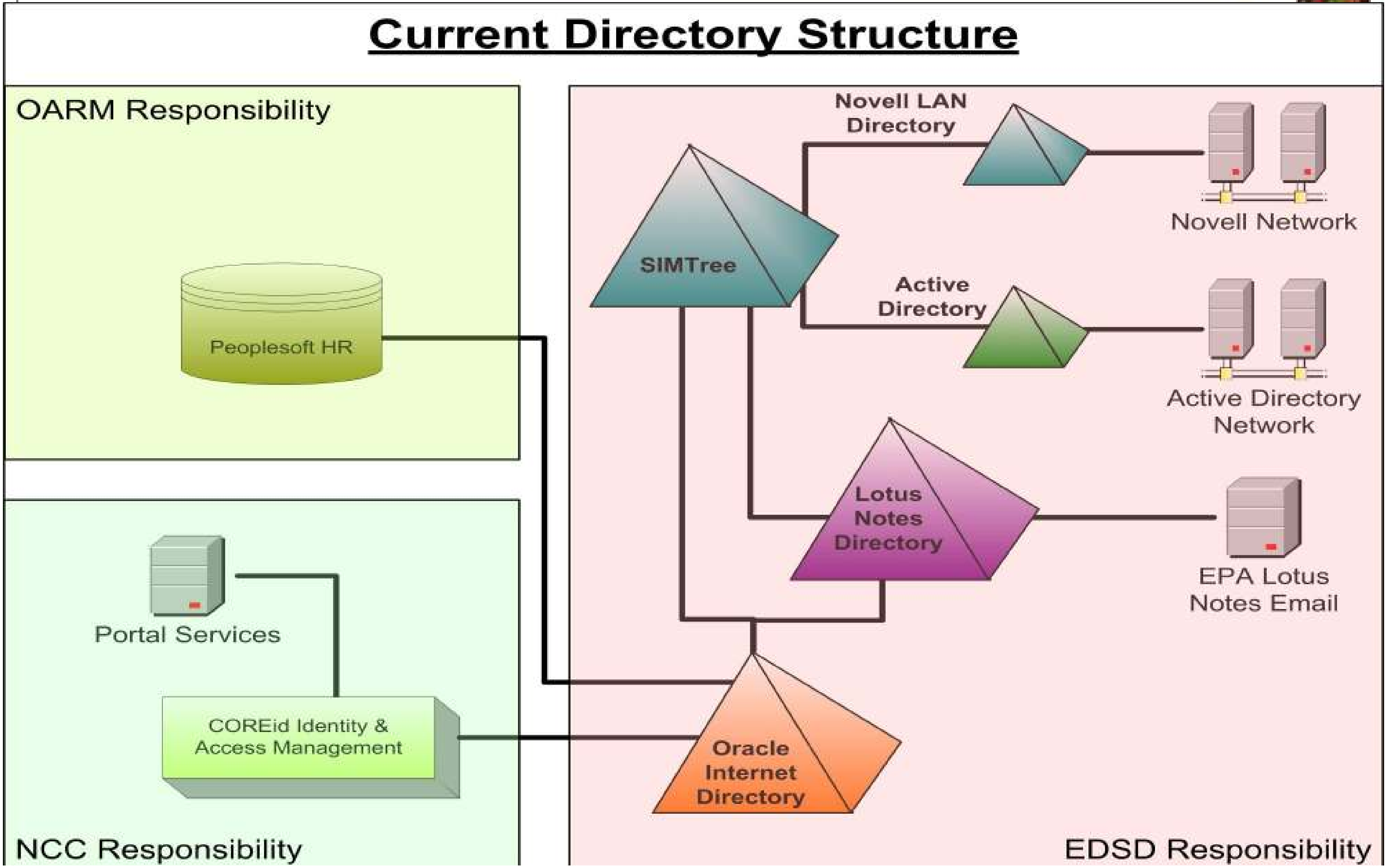
[1] Source: “Password Management, Single Sign-on, and Authentication Management Infrastructure Products: Perspective,” Ant Allan, Gartner Technology Overview, January 7, 2003.

[2] Source: “Intranet Access Management”, Microsoft, July 2004.

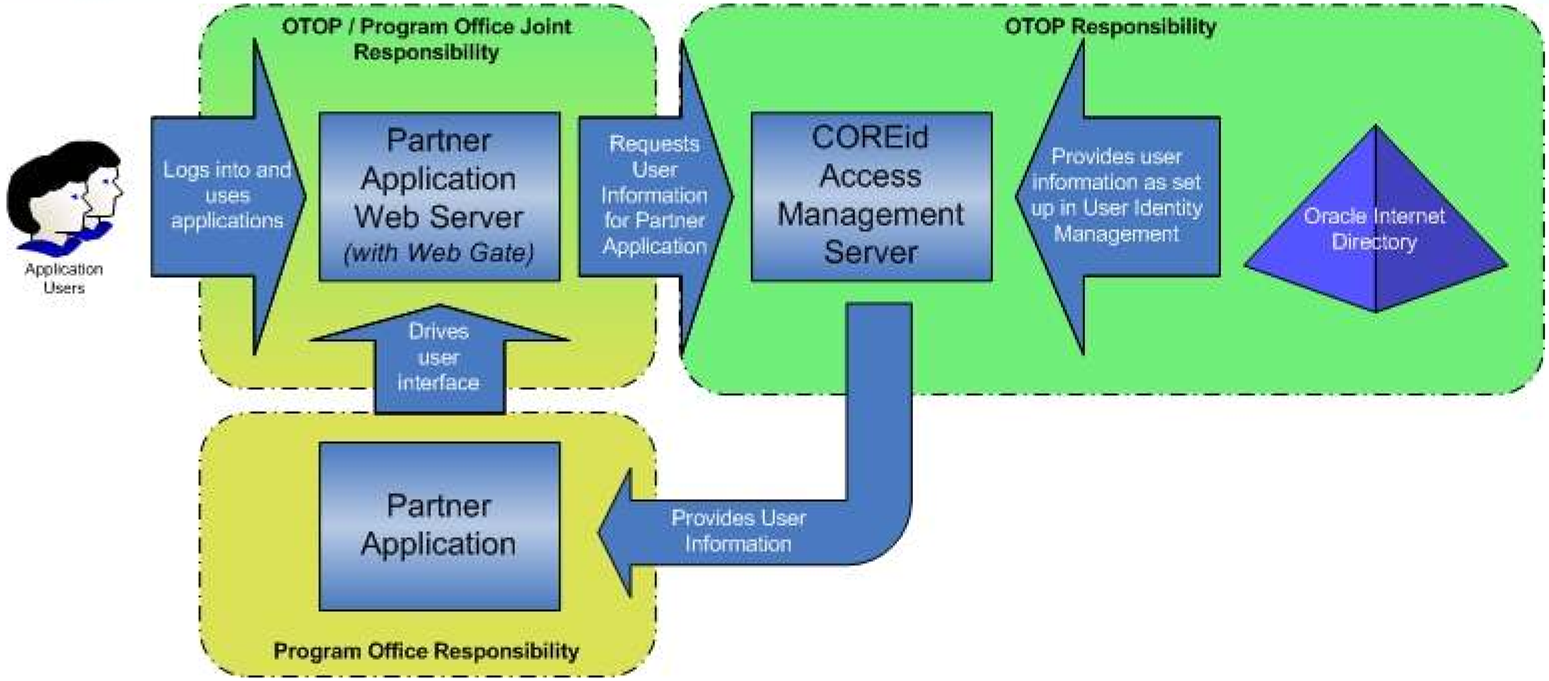
EPA User Definitions

- **EPA Employees** – People who are hired by the EPA
- **Inside Affiliates** – On-site Contractors
- **External User** – Anyone who works on behalf of EPA for compensation, but does not have an EPA email address, including off-site contractors, environmental laboratory technicians, etc. Also includes business partners who work in conjunction with EPA, including researchers, regulated industry, other government officials, etc.

Directory Synchronization

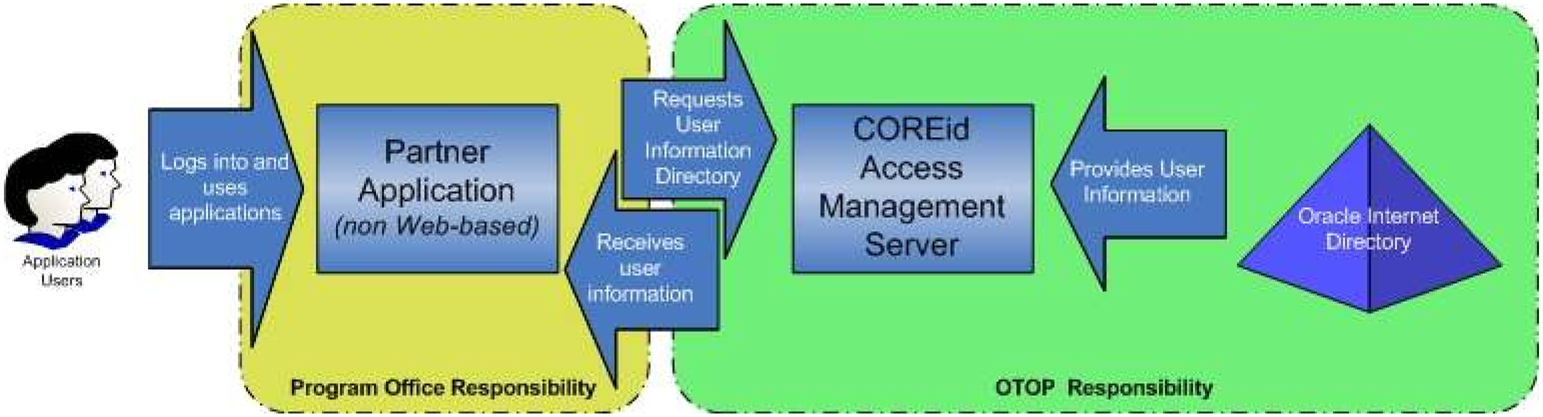


Access Control: Web Single Sign-on


OTOP / Program Office Joint Responsibility
OTOP Responsibility
Application Users
Logs into and uses applications
Partner Application Web Server (with Web Gate)
Requests User Information for Partner Application
COREid Access Management Server
Provides user information as set up in User Identity Management
Oracle Internet Directory
Drives user interface
Partner Application
Provides User Information
Program Office Responsibility

- Web Access Management is controlled by the Partner Application's Web server:
  - The server is equipped with a plug-in called a Web Gate
  - The Web Gate requests user information for the Partner application
  - All data about users comes from the Oracle Internet Directory

Access Control: Application Single Sign-on


Application Users
Logs into and uses applications
Partner Application (non Web-based)
Requests User Information Directory
Receives user information
COREid Access Management Server
Provides User Information
Oracle Internet Directory
Program Office Responsibility
OTOP Responsibility

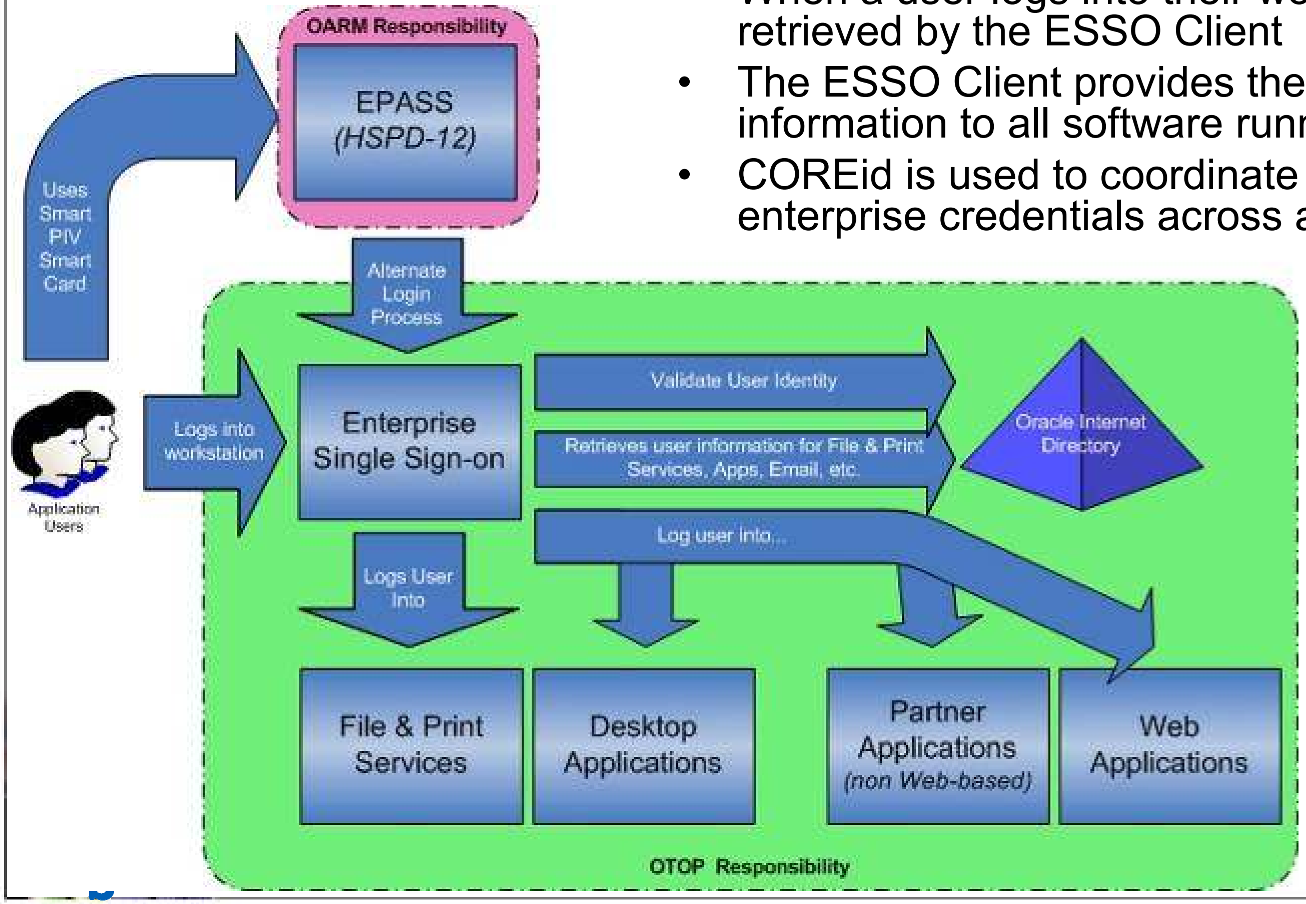
- For non Web-based applications, the process is more direct:
  - The Partner Application requests user information from the COREid Access Management Server via web services
  - User information and access rights are received via the web services

ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

Access Control: Enterprise Single Sign-on

- Enterprise Single Sign-on (ESSO) relies on software on the client computer to coordinate user credentials:
  - User Identity and Access information is stored in the Oracle Internet Directory
  - When a user logs into their workstation, their identity is retrieved by the ESSO Client
  - The ESSO Client provides the identity and access information to all software running on the workstation
  - COREid is used to coordinate provisioning of enterprise credentials across all services and apps



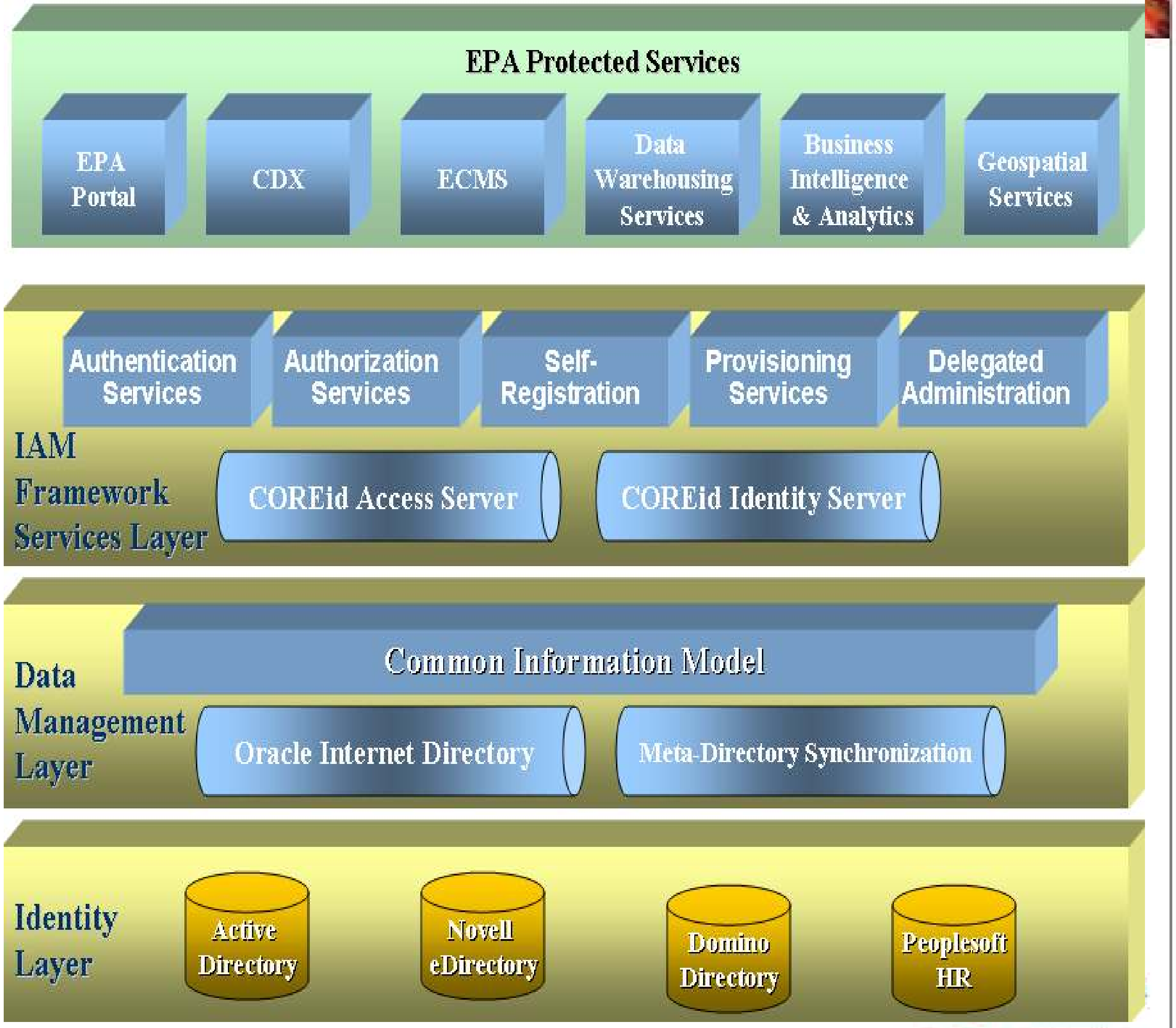
Lesson 5: The EPA Enterprise WAM Architecture

OFFICE OF ENVIRONMENTAL INFORMATION

EPA WAM Conceptual Architecture

WAM Layered Architecture:

- **EPA Protected Services** – The systems that are being protected
- **WAM Framework Service Layer** – Provides business services to protect EPA applications
- **Data Management Layer** – Provides a common information model to aggregate user and group attributes.
- **Identity Layer** – EPA's authoritative data sources.



EPA Protected Services

EPA Portal

CDX

ECMS

Data Warehousing Services

Business Intelligence & Analytics

Geospatial Services

IAM Framework Services Layer

Authentication Services

Authorization Services

Self-Registration

Provisioning Services

Delegated Administration

COREid Access Server

COREid Identity Server

Data Management Layer

Common Information Model

Oracle Internet Directory

Meta-Directory Synchronization

Identity Layer

Active Directory

Novell eDirectory

Domino Directory

Peoplesoft HR

ENTERPRISE TOOLS WORKSHOP

Oracle Access Management Suite

- Oracle Internet Directory (LDAP Server)
- Oracle Directory Integration Platform
  - Performs synchronization and integration across various directories
- Oracle Access Manager
  - formerly Oracle COREid Access and Identity
  - provides identity administration, and access control to Web applications and resources
  - provides the user and group management, delegated administration, password management and self-service functions
  - Includes Oracle WebGate - a web server plug-in access client that intercepts HTTP requests for protected resources and forwards them to the Access Server.
- Oracle Identity Manager
  - automates user provisioning, identity administration, and password management, wrapped in a comprehensive workflow engine
  - Includes Oracle WebPass – a web server plug-in that passes information back and forth between a web server and the Identity Server.

Framework Services

- Authentication Manager
  - Generate and validate SSO tokens
  - Retrieve userID from a given SSO token
- User Service
  - Read/Write and manipulate User information
  - Uses WAM Request and Response objects for interface flexibility
- Group Manager
  - Read user group data, including members
  - New groups still need to go through NCC processes to be created

- Note: We will go more in detail about these services in the lab.

Framework Services (cont'd)

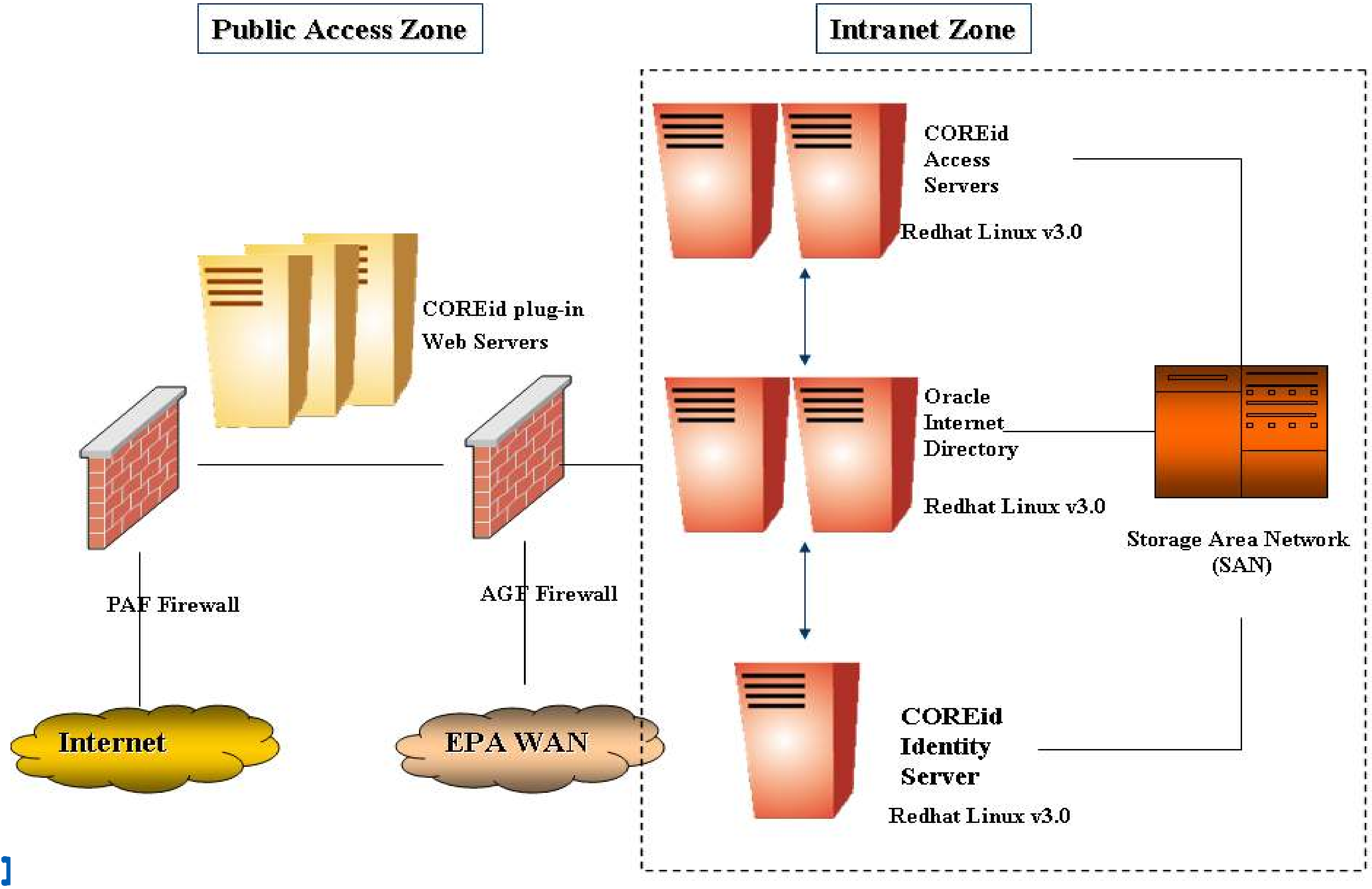
- Delegated Administration Service
  - Process pending Self-Registration and Subscribe To Group requests
  - Add members or owners to groups
- Provisioning Service
  - Subscribe and Un-subscribe from groups
- Self Service
  - Self-Register, change your password and retrieve userid based on e-mail address

- Note: These services are not covered in the lab. To learn more about them, contact the WAM team

Lesson 6: The Enterprise WAM in Production

OFFICE OF ENVIRONMENTAL INFORMATION

WAM Production Diagram



Public Access Zone

Intranet Zone

COREid Access Servers

Redhat Linux v3.0

COREid plug-in Web Servers

Oracle Internet Directory

Redhat Linux v3.0

Storage Area Network (SAN)

PAF Firewall

AGF Firewall

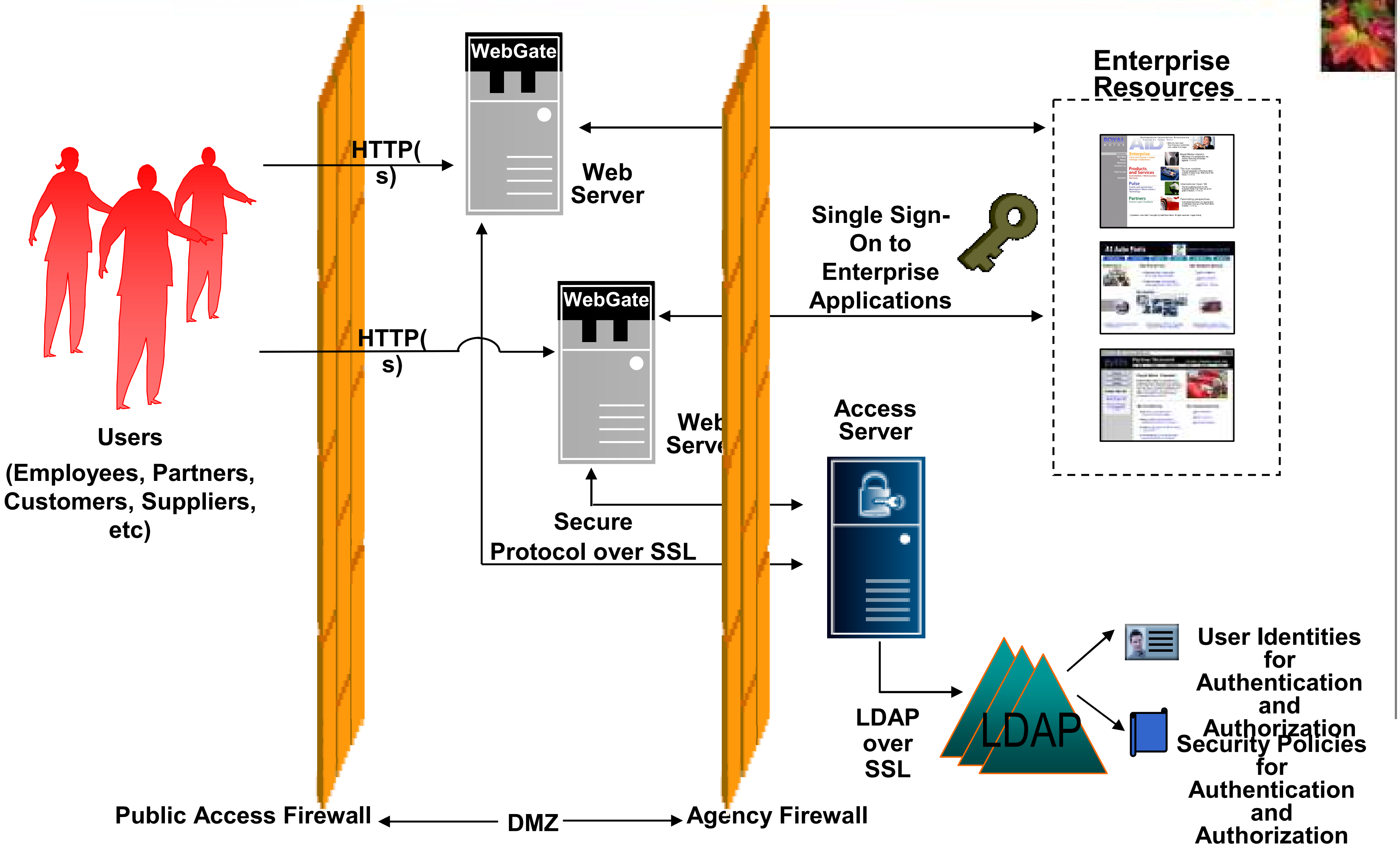
Internet

EPA WAN

COREid Identity Server

Redhat Linux v3.0

OAM Access Management Overview



Enterprise Resources

WebGate

HTTP(s)

Web Server

Single Sign-On to Enterprise Applications

WebGate

HTTP(s)

Web Serve

Users (Employees, Partners, Customers, Suppliers, etc)

Access Server

Secure Protocol over SSL

LDAP over SSL

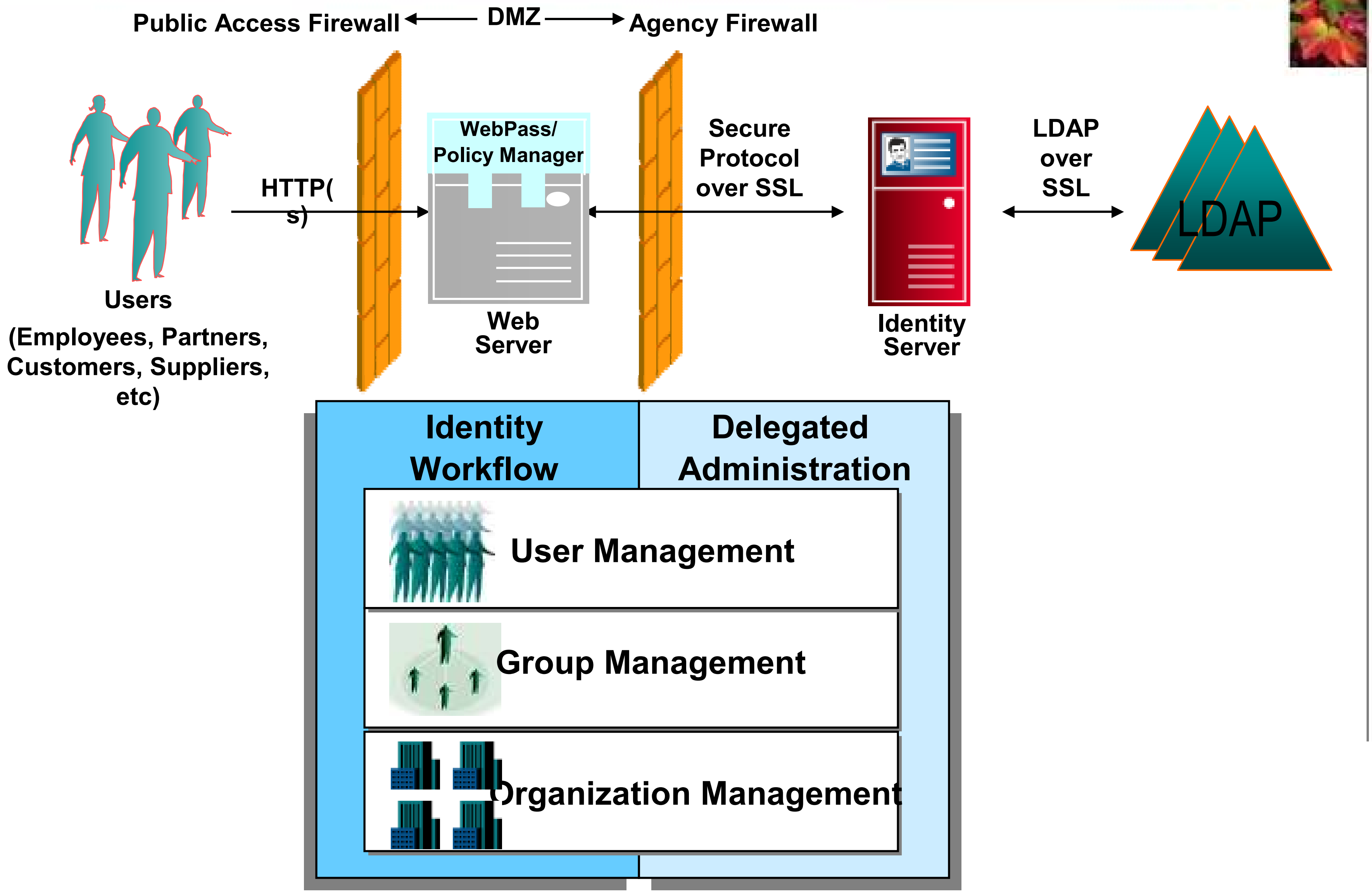
LDAP

User Identities for Authentication and Authorization

Security Policies for Authentication and Authorization

Public Access Firewall ← DMZ → Agency Firewall

OAM Identity Management Overview



Public Access Firewall ← DMZ → Agency Firewall

Users

(Employees, Partners, Customers, Suppliers, etc)

HTTP(s)

WebPass/ Policy Manager

Web Server

Secure Protocol over SSL

Identity Server

LDAP over SSL

LDAP

Identity Workflow

Delegated Administration

User Management

Group Management

Organization Management

Lesson 7: Standards and compliance

OFFICE OF ENVIRONMENTAL INFORMATION

Security Standards

- System security should be addressed during each phase of the development life cycle
- It is critical for a WAM Integration effort to identify the security controls that should be applied
- The Security Controls - Management, Operational and Technical should be documented
- System Owners will need specifically to determine their system requirements for confidentiality, integrity and availability

Security Standards (cont)

- The WAM's security controls will be elevated in the event that an integrating application has HIGH confidentiality, integrity or availability ratings
- The EPA Information Security Manual 2195A1 aligns with generally accepted National Institute of Standards and Technology (NIST) standards and guidelines
- NIST Security Standards should be reviewed for applicable security standards to be applied to development throughout the system life cycle

ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

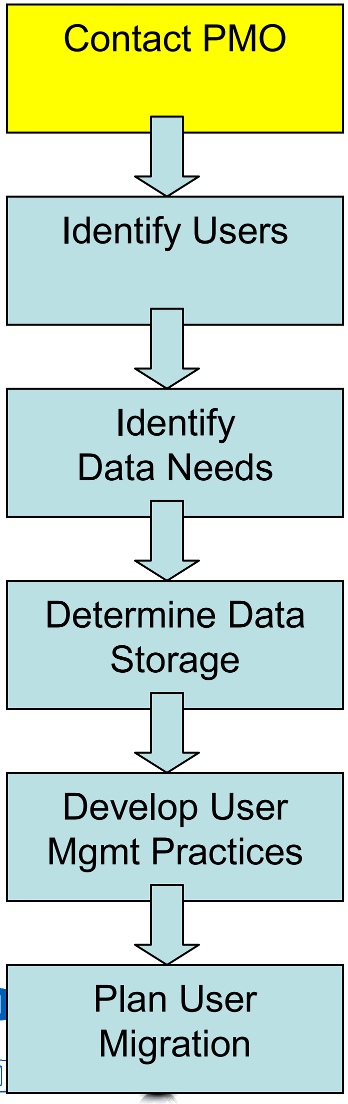
Security Standards: Applicable NIST Security Standards

NIST Publication	Name
NIST SP 800-64	Security Considerations in the Information System Development Life Cycle
NIST SP 800-61	Computer Security Incident Handling Guide
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
NIST SP 800-57	Recommendation on Key Management
NIST SP 800-56	Recommendation on Key Establishment Schemes
NIST SP 800-55	Security Metrics Guide for Information Technology Standards
NIST SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
NIST SP 800-53	Security Controls for Federal Information Systems
NIST SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
NIST SP 800-47	Security Guide for Interconnecting Information Technology Standards
NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
NIST SP 800-36	Guide to Selecting Information Technology Security Products
NIST SP 800-35	Guide to Information Technology Security Services
NIST SP 800-34	Contingency Planning Guide for Information Technology Systems
NIST SP 800-31	Intrusion Detection Systems (IDS)
NIST SP 800-30	Risk Management Guide for Information Technology Systems
NIST SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
NIST SP 800-26	Security Self-Assessment Guide for Information Technology Systems
NIST SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition / Use of Tested/Evaluated Products
NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-12	An introduction to Computer Security: The NIST Handbook
NIST FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
NIST FIPS 140-2	Security Requirements for Cryptographic Modules

Lesson 8: WAM Integration Process

OFFICE OF ENVIRONMENTAL INFORMATION

Integration Overview



Contact PMO

Identify Users

Identify Data Needs

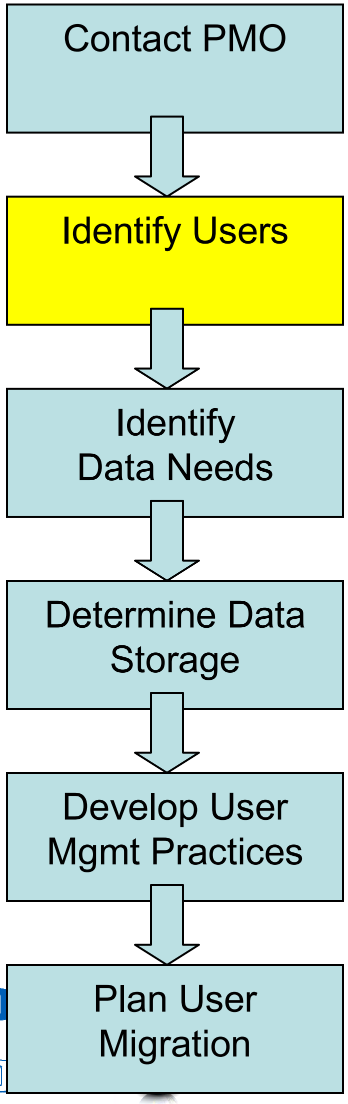
Determine Data Storage

Develop User Mgmt Practices

Plan User Migration

- **Maja Lee** - Directly responsible for the implementation of the WAM system
  - Coordinates data needs to ensure consistent, non-repetitive data in the Oracle Internet Directory
  - Executes MOUs to ensure that all security policies are understood and agreed to
  - Schedules changes to the WAM system to avoid conflicts and minimize downtime
  - Reviews all system updates to ensure compatibility across partner systems
  - Provides technical support services and training
  - Conduct Design Review Meeting
  - Fill out Interface Control Document (ICD)

Integration Overview


Contact PMO

Identify Users

Identify Data Needs

Determine Data Storage

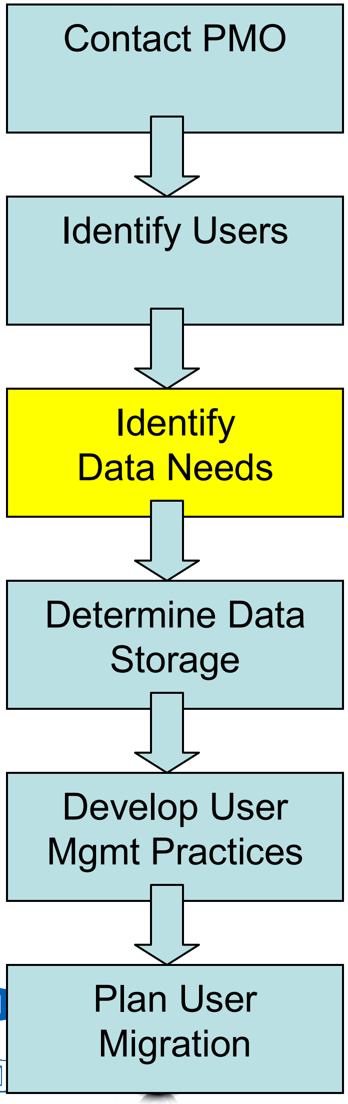
Develop User Mgmt Practices

Plan User Migration

❖ Identify Users

- Determine the end users of the application
- Map users to their respective types in WAM (internal, inside affiliate, external)
- Identify any orphan user classes and work with PMO to address concerns

Integration Overview



Contact PMO

Identify Users

Identify Data Needs

Determine Data Storage

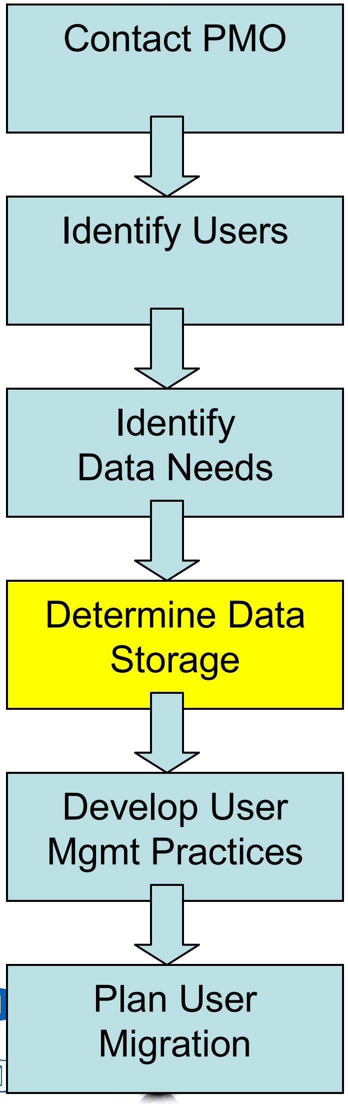
Develop User Mgmt Practices

Plan User Migration

❖ Identify Data Needs

- For each user class, what information do you need to know about a specific user
- What information is not already provided by the base users classes
- Refer to current OID Data Dictionary available from PMO for base user class definitions

Integration Overview



Contact PMO

Identify Users

Identify Data Needs

Determine Data Storage

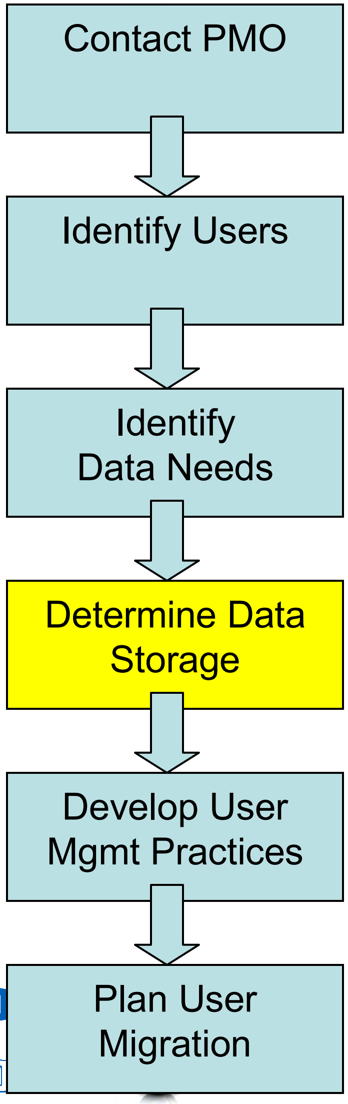
Develop User Mgmt Practices

Plan User Migration

❖ Determine Data Storage

- If there is data not provided by the base users classes, where to store that data?
- Are there different storage needs dependent on the different types of users?
- How to link user data to system data?

Where to Store Application Specific Data: Store Locally



Contact PMO

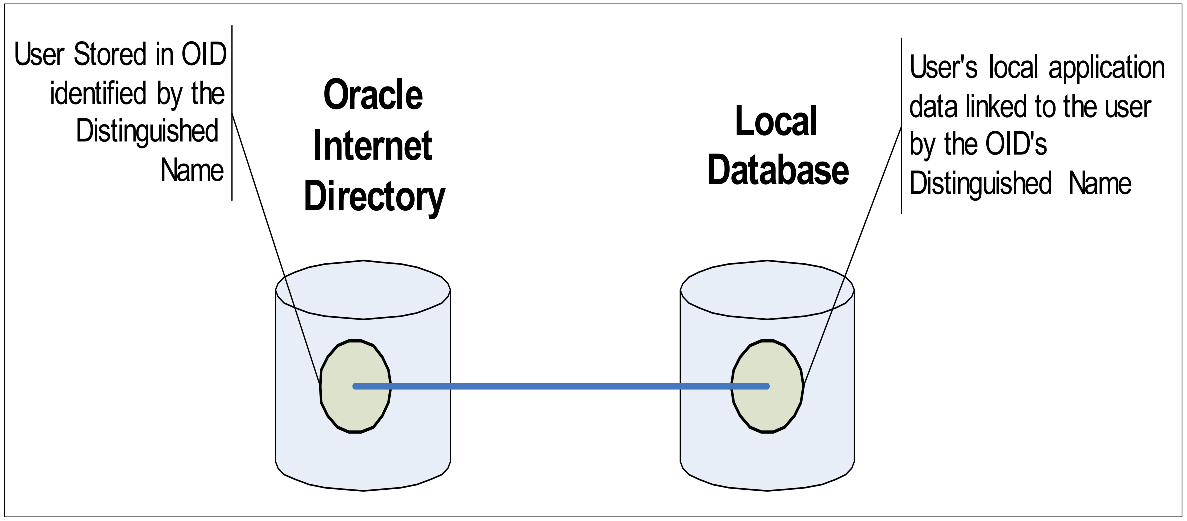
Identify Users

Identify Data Needs

Determine Data Storage

Develop User Mgmt Practices

Plan User Migration



User Stored in OID identified by the Distinguished Name

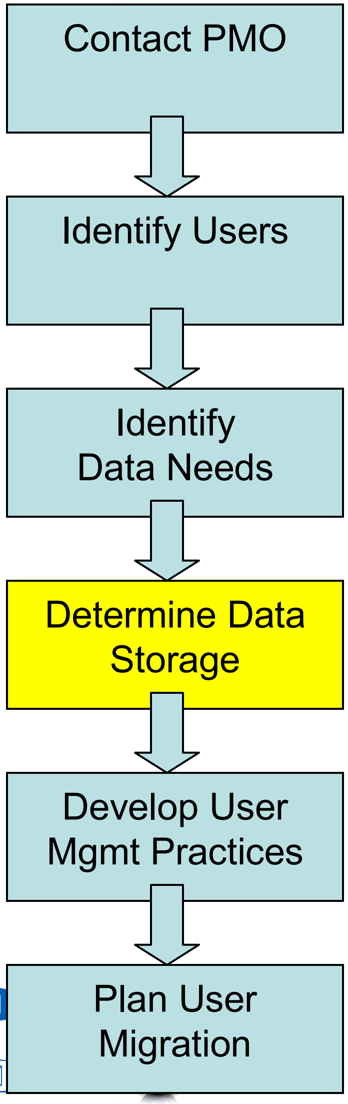
Oracle Internet Directory

Local Database

User's local application data linked to the user by the OID's Distinguished Name

- In the application database using unique user key
  - User specific application data can be locally stored and link to WAM through the Distinguished Name field

Where to Store Application Specific Data: Extend CoreID


Contact PMO

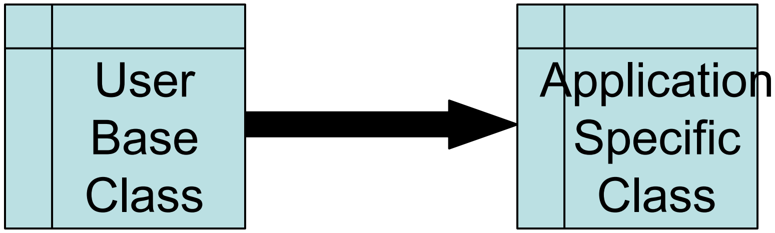
Identify Users

Identify Data Needs

Determine Data Storage

Develop User Mgmt Practices

Plan User Migration


User Base Class

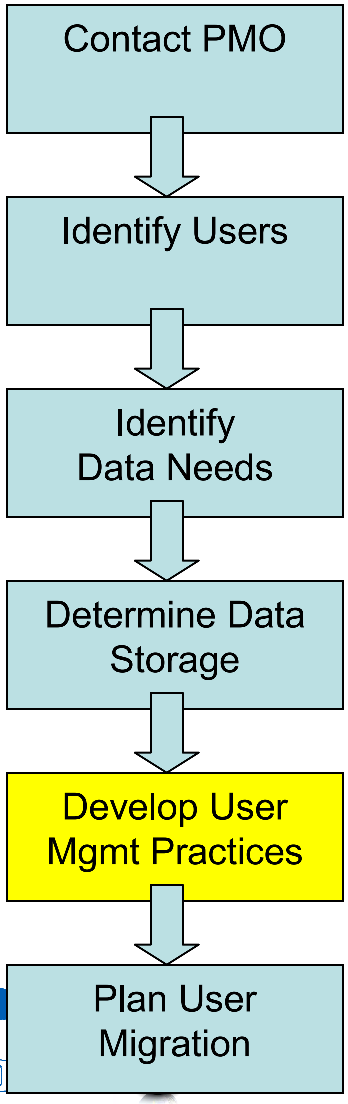
Application Specific Class

A user's base class can be either:
-EPA Employee
-Inside Affiliate
-External User

The Application Specific class is used to extend the base class to include Data needed by a single application or group of apps.

- Extend the OID user classes
  - Additional application data fields are added to OID by adding additional data classes
  - Attaching the different data classes to a specific user extends that user's information to provide the specific application data

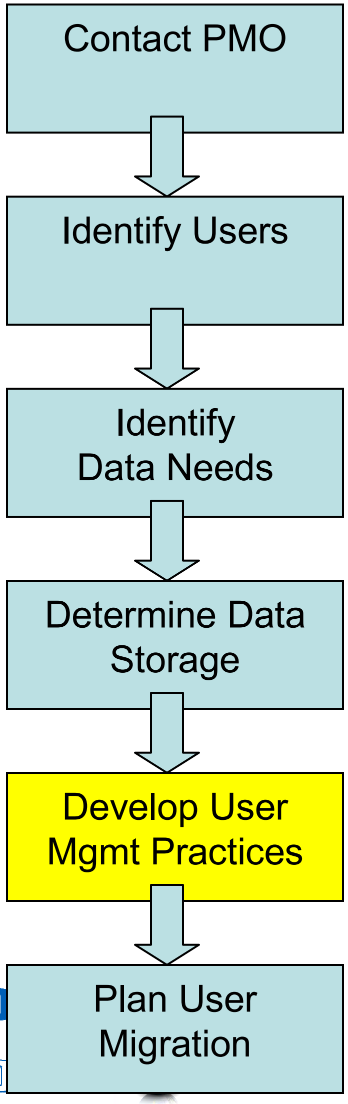
Integration Overview



❖ Develop User Management Practices

- Use the COREid Tools to manage user information?
- Develop custom processes via WAM Web Services?
- Develop custom processes through COREid API?
- Direct LDAP integration with OID?

Integration Overview



❖ COREid Tools

+ Quickest time to implement

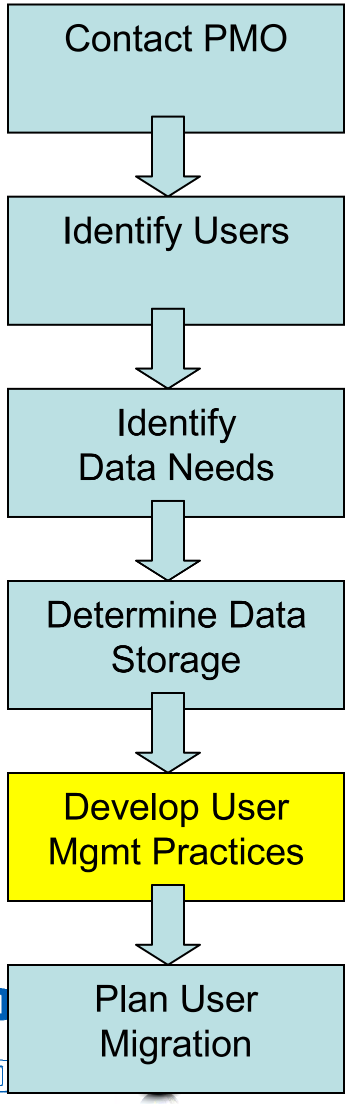
+ Provides a robust environment for user management

+ PMO Preferred Approach

- Requires re-training of user administrators

- Limited ability for end users to self-administer

Integration Overview



❖ WAM Web Services

+ Easy to implement using XML-based services

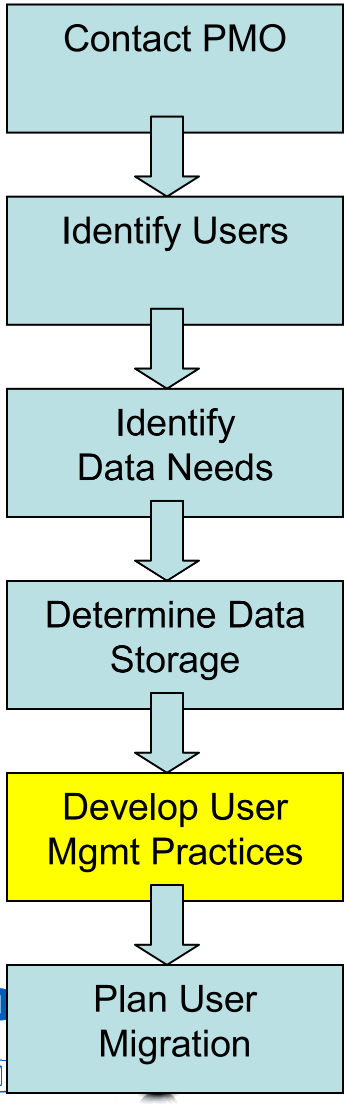
+ Provides wide range of functionality

+ Minor modifications possible to accommodate special requirements

+ PMO Preferred Alternate Approach

- Requires more effort on the part of OEI and Program Offices to implement

Integration Overview



Contact PMO

Identify Users

Identify Data Needs

Determine Data Storage

Develop User Mgmt Practices

Plan User Migration

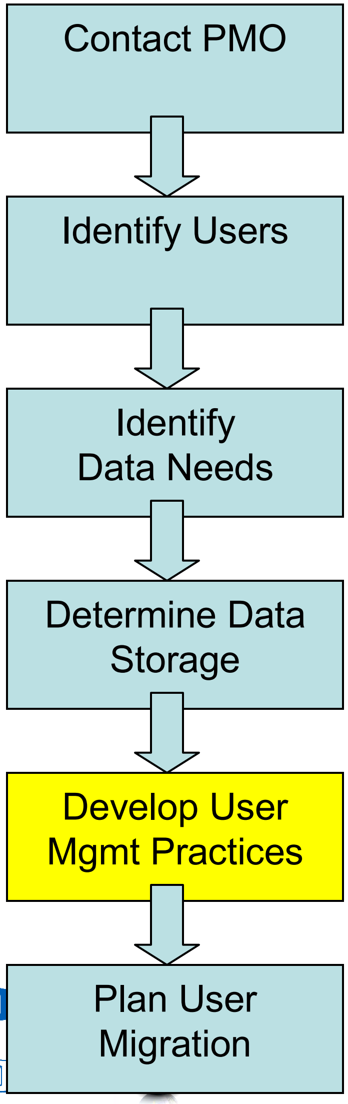
❖ COREid API

+ Provides significant customization opportunities

- API requires specialized development training

- Requires additional security and integration reviews and testing

Integration Overview



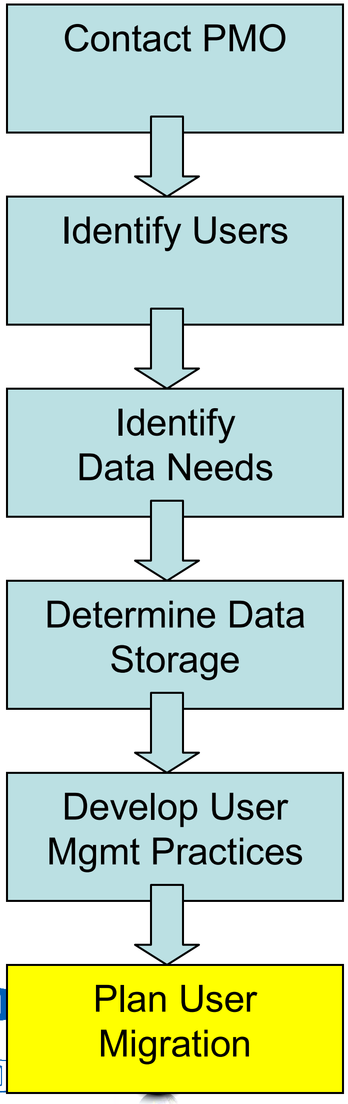
LDAP Integration with OID

+ May be only viable option for some COTs

- LDAP query language requires specialized development skills

- Requires extensive security and interoperability review and oversight to limit liabilities to WAM and partner systems

Integration Overview



Plan User Migration

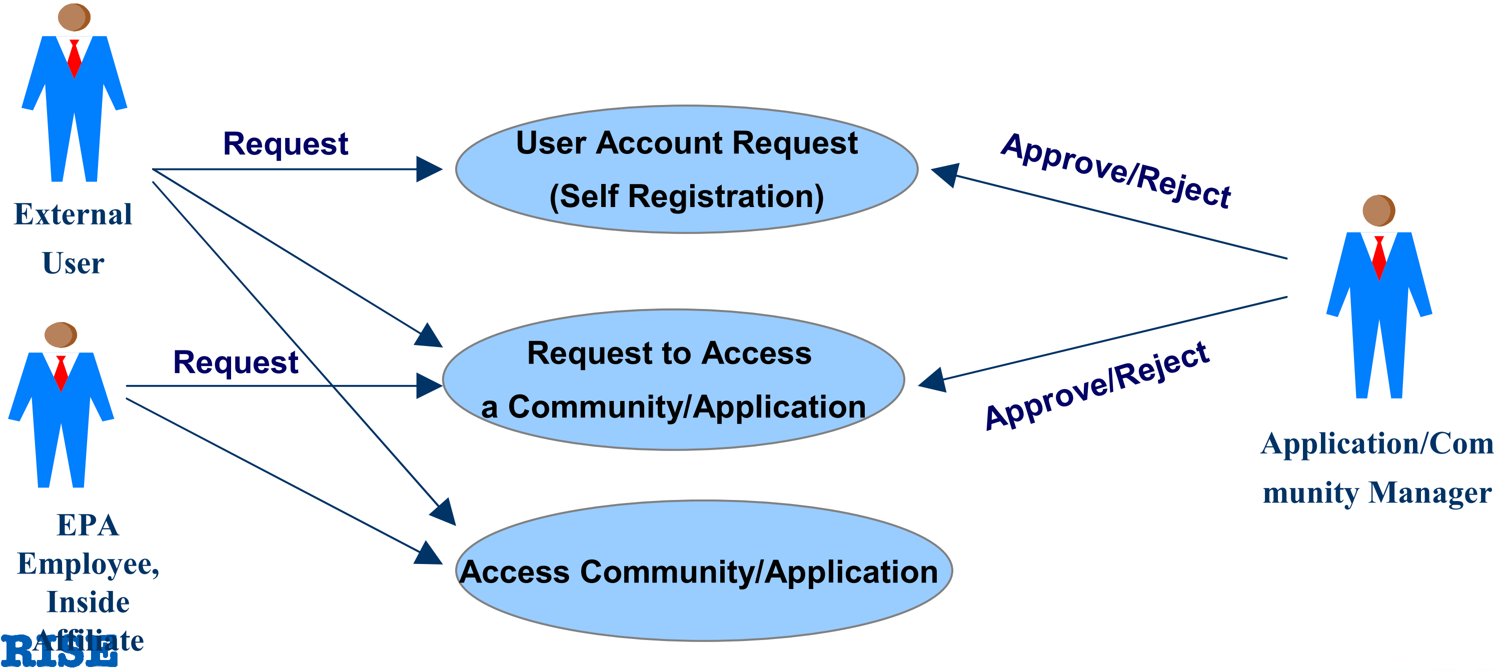
- Determine how many user accounts need to be migrated to the OID
- Map data fields
- PMO can assist in writing data migration scripts
- How will users be notified of changes to account?
- Will users need to re-subscribe to maintain their account?

Lesson 9: EPA WAM and EPA Portal together

OFFICE OF ENVIRONMENTAL INFORMATION

Users

- Self Registration
- Request Access to a Community



External User

Request

User Account Request (Self Registration)

Approve/Reject

EPA Employee, Inside Affiliate

Request

Request to Access a Community/Application

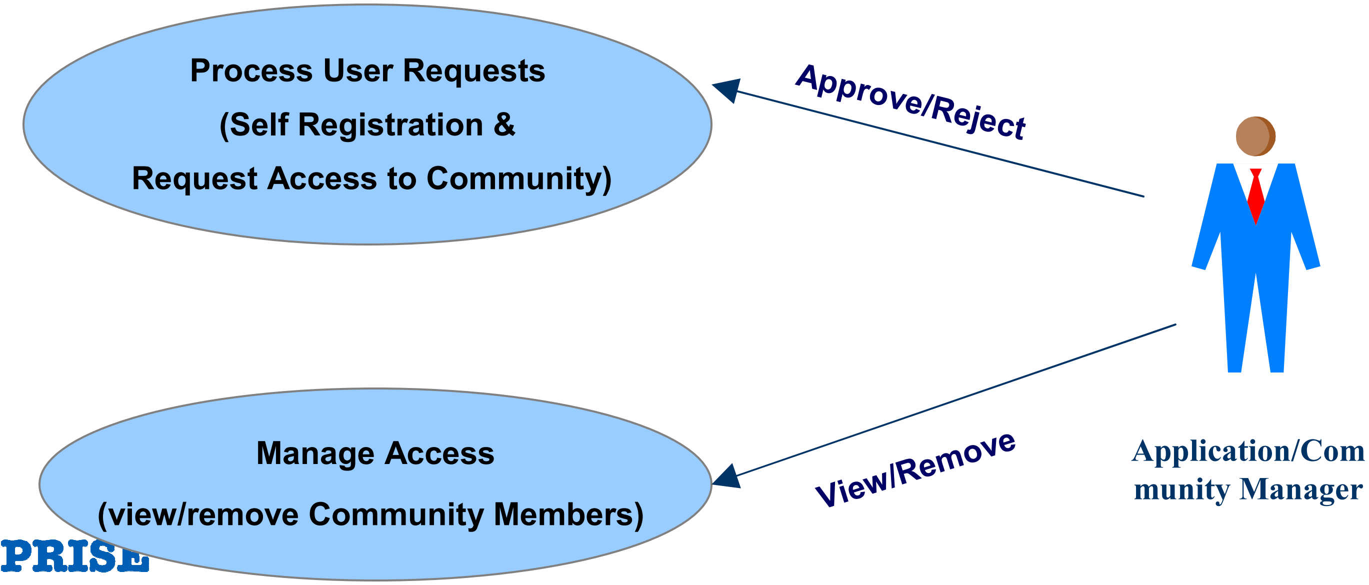
Approve/Reject

Access Community/Application

Application/Com munity Manager

Community/Application Managers

- Process user requests for access to community
- Manage access to community



Process User Requests (Self Registration & Request Access to Community)

Manage Access (view/remove Community Members)

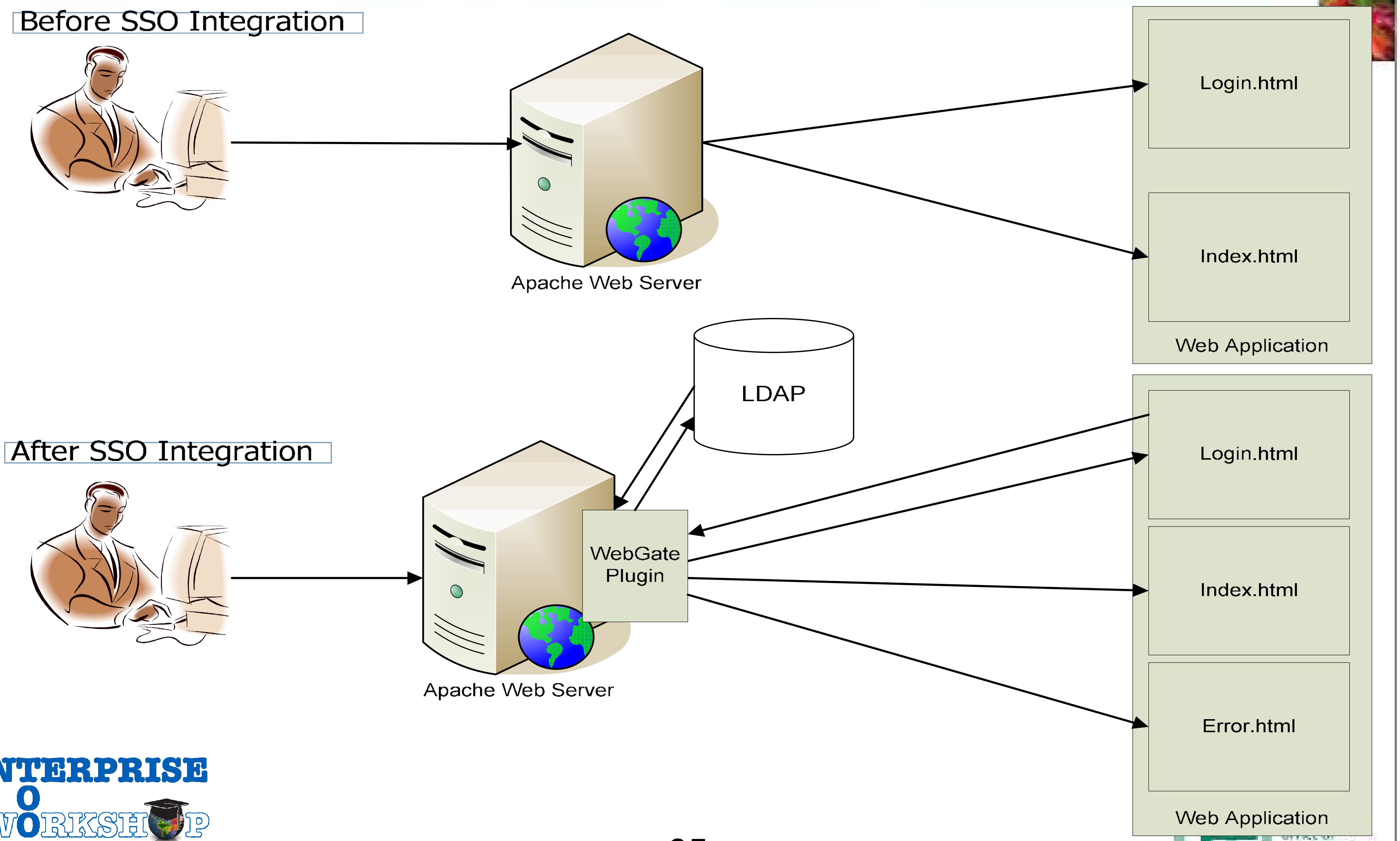
Lesson 10: Lab

OFFICE OF ENVIRONMENTAL INFORMATION

Overview

- Web Single Sign-On Integration
  - Deploy a simple web application onto Apache web server
  - Secure that application by installing Oracle WebGate
  - Confirm SSO to Portal
- WAM Web Services Integration
  - Use Eclipse to write sample code to call WAMFW web services

Web Single Sign-On Integration



Before SSO Integration

Apache Web Server

Login.html

Index.html

Web Application

LDAP

After SSO Integration

WebGate Plugin

Apache Web Server

Login.html

Index.html

Error.html

Web Application

Oracle Access Manager Administration

- To protect an application using Oracle Access Manager and WebGate, a Policy Domain must be established

- A Policy Domain encompasses:
  - Resources you want to protect
  - Policies for protection
  - Rules for protection
    - Authentication, Authorization and Audit rules

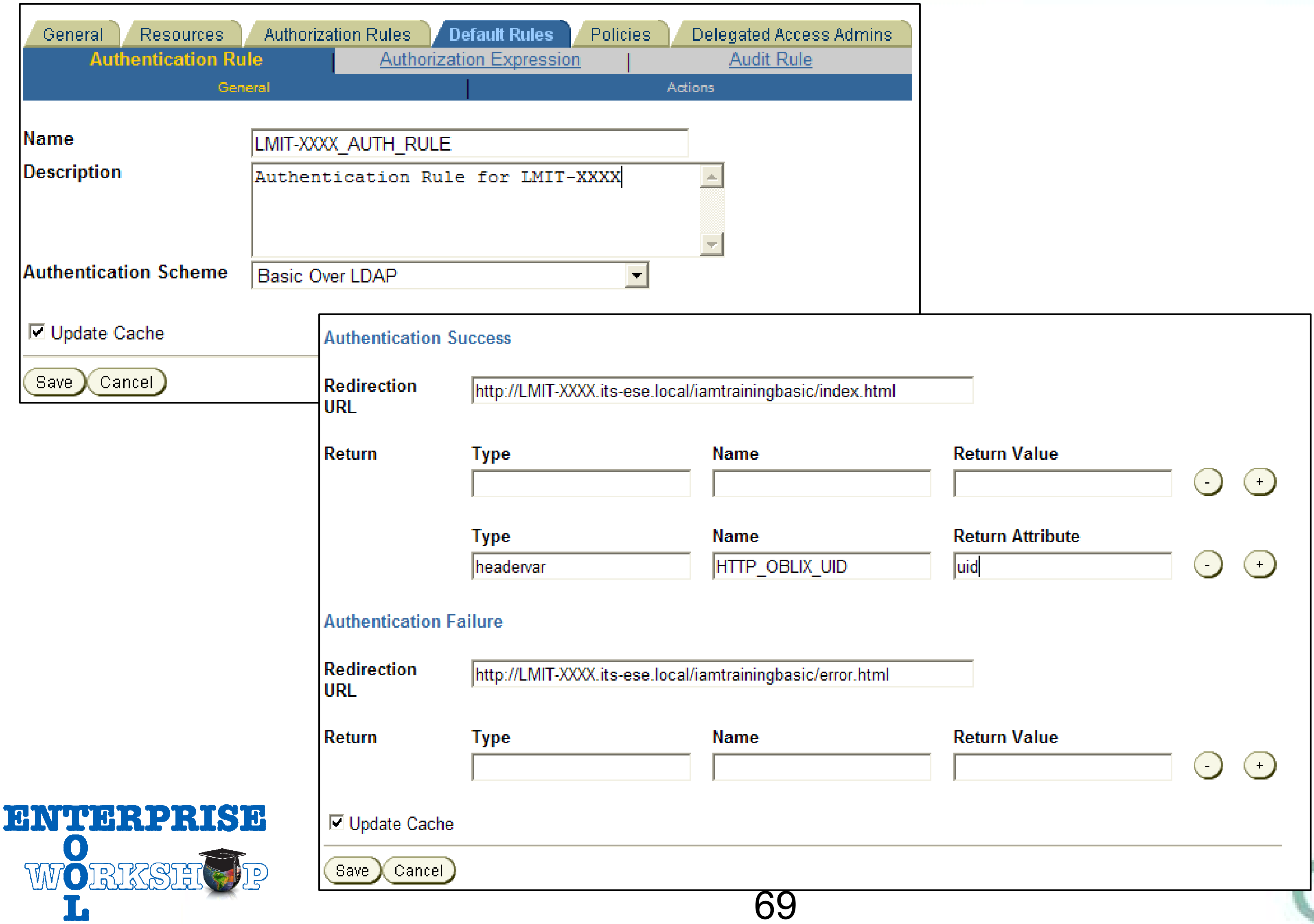
Policy Domain – Resources and Policies

- Resources defined in the Policy domain:
  - Can be web or non-web (urls, ejbs, documents)
  - Act hierarchically
- A Policy is a way to break the policy domain into smaller pieces using:
  - Resource types
  - Resource Operations
  - Resources (defined above)
  - Host Identifiers
- Any number of Policies can be created using combinations of those items

Rules for Protection - Authentication

- Specifies the Authentication Scheme to be used
  - Defines how the user will be challenged for credentials
  - Basic and Anonymous Authentication schemes are provided by Oracle.
- Specifies which actions should be taken when authentication succeeds or fails.
  - Redirection
  - HTTP Header variables
    - Values can be static or OID attributes
  - Cookies
    - Values can be static or OID attributes

Authentication Rule setup



Name	LMIT-XXXX_AUTH_RULE
Description	Authentication Rule for LMIT-XXXX
Authentication Scheme	Basic Over LDAP

☑ Update Cache

Authentication Success

Redirection URL: http://LMIT-XXXX.its-ese.local/iamtrainingbasic/index.html

Return	Type	Name	Return Value

Type	Name	Return Attribute
headervar	HTTP_OBLIX_UID	uid

Authentication Failure

Redirection URL: http://LMIT-XXXX.its-ese.local/iamtrainingbasic/error.html

Return	Type	Name	Return Value

☑ Update Cache

Rules for Protection – Authorization

- Establish timing conditions for access
- Establish actions to be taken on success and failure
  - Same options as Authentication actions
- Allow and Deny Access
  - Based on specific OID users, roles, IP Addresses or LDAP filtering
  - Can configure which of these takes precedence
- More than one Authorization rule can be used in a Policy
  - Logically concatenated into AuthZ Expressions

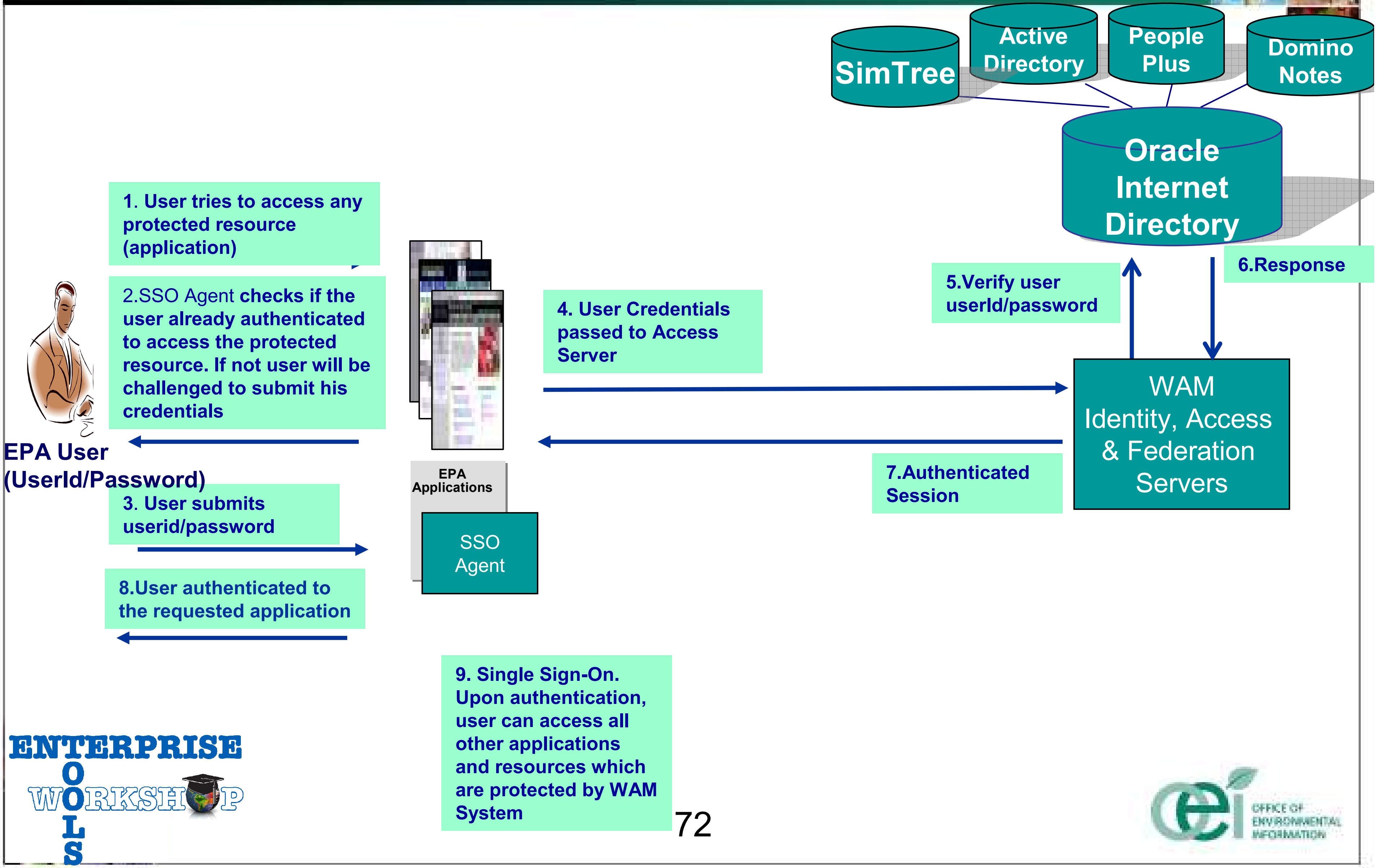
ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

SSO Lab

1. Deploy the html files into Apache
2. Confirm access to all html pages is open
3. Click on link to Portal, confirm lack of SSO
4. Install WebGate, configure using pre-defined Access Gate configuration
5. Restart Apache
6. Access html pages
7. Login
8. Click on link to Portal, confirm SSO

Web Single Sign-On Integration



SimTree

Active Directory

People Plus

Domino Notes

Oracle Internet Directory

1. User tries to access any protected resource (application)

2.SSO Agent checks if the user already authenticated to access the protected resource. If not user will be challenged to submit his credentials

EPA User (UserId/Password)

3. User submits userid/password

4. User Credentials passed to Access Server

5.Verify user userId/password

6.Response

7.Authenticated Session

8.User authenticated to the requested application

9. Single Sign-On. Upon authentication, user can access all other applications and resources which are protected by WAM System

ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION

WAM Web Services

- To be used within individual applications to:
  - Read centralized user and group information
    - Last name, first name, phone number, etc
    - User Type booleans
    - Group Members
  - Modify centralized user information
  - Subscribe and unsubscribe to existing groups
  - Add members and owners to existing groups
  - Read and process pending access requests
  - Change a user’s password

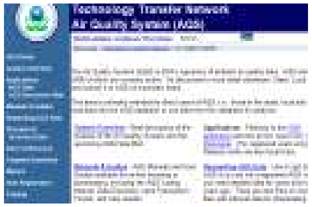
WAM Web Services Integration

EPA Applications

Welcome to the EPA Portal

My Page

Welcome to the EPA Portal


Technology Transfer Network

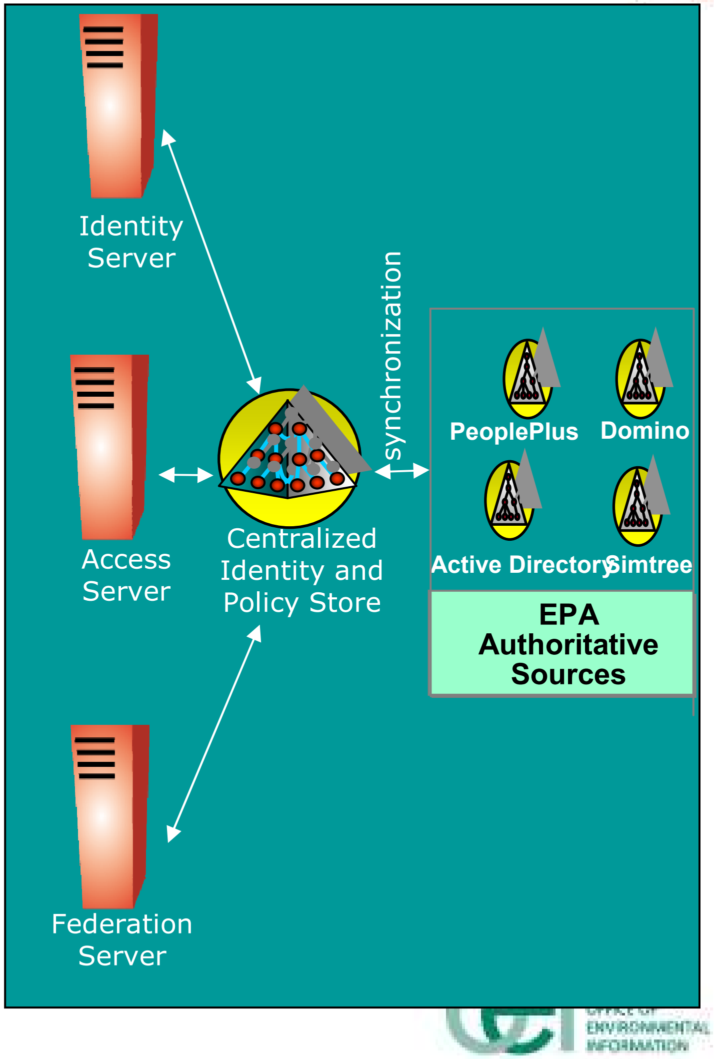
Air Quality System (AQS)

EPA Search Results

WAM Web Services

- Authentication Services
- Self Registration Services
- User Management Services
- Group Management Services
- Provisioning Services
- Delegated Administration Services
- Policy Management Services

WAM Infrastructure



Instantiating Web Services in Java

- All endpoints can be setup using the WAMLocator class in the WAMFW client jar

```
gov.epa.iamfw.client.WAMLocator;
gov.epa.iamfw.webservices.auth.AuthMgr;
gov.epa.iamfw.webservices.userservice.UserService
gov.epa.iamfw.webservices.group.GroupMgr;
gov.epa.iamfw.webservices.delegatedAdministration.DelegatedAdministrationService;
gov.epa.iamfw.webservices.selfService.SelfService;
gov.epa.iamfw.webservices.provisioning.ProvisioningService;


WAMLocator iamLocator = WAMLocator.getInstance
            ("http://ese-ut.its-ese.local:7778/iamfw/services");
AuthMgr = iamLocator.getAuthMgr();
```

Calling Web Service methods

- Authentication Token
  - Must be generated using AuthMgr and passed on calls to all other web services
- Request and Response objects
  - Newer services require WAM Request objects to be built and passed as the only argument to each method.
  - Unique to the method being called, but inherit from the same object
  - Allow for modification of the web service arguments without having to change code in the applications which use them

Web Service call example

```
WAMLocator iamLocator = WAMLocator.getInstance
        ("http://ese-ut.its-ese.local:7778/iamfw/services");
authMgr = iamLocator.getAuthMgr();
userSvc = iamLocator.getUserService();

String token = authMgr.authenticate(user, passwd,
     gov.epa.iamfw.webservices.common.AuthMethod.password);
Request request = new Request();
request.setToken(token);
request.setUserId(user);

Response response = userSvc.getUser(request);
if (response != null ){
              System.out.println( response.getUserProfile().getFirstName()[0] );
              System.out.println( response.getUserProfile().getLastName()[0] );
}
```

Lab – Web Services Integration

1. Create a new Eclipse workspace
2. Unpack the iamfwclient.jar file into workspace
3. Create classes and test out web service access using iamlabXX users

Lesson 11: Course Wrap-up

OFFICE OF
ENVIRONMENTAL
INFORMATION

Overview

- Course Review
- What’s Next?

Course Review

- Lesson 1: Welcome and Course Overview
- Lesson 2: WAM Concepts and Definitions
- Lesson 3: The EPA Enterprise WAM System
- Lesson 4: The EPA Enterprise WAM Architecture
- Lesson 5: The EPA WAM System in production
- Lesson 6: Standards and compliance
- Lesson 7: The EPA WAM Integration Process
- Lesson 8: EPA WAM and EPA Portal together
- Lesson 9: Lab

What’s Next?

- You are Members of EPA’s WAM Development Community! This means that you will:
  - Be able to participate in development standards discussions
  - Be able to share the details of projects they are working on
  - Be able to get help to issues that they encounter in their development
  - Be able to provide help to others
- You are ambassadors to your clients!
  - Tech your clients about the EPA WAM and what is out there

End of Course

- Thank you for your time!

ENTERPRISE TOOLS WORKSHOP

OFFICE OF ENVIRONMENTAL INFORMATION